

**MEMORANDUM OF UNDERSTANDING BETWEEN
THE DEPARTMENT OF HOMELAND SECURITY,
IMMIGRATION AND CUSTOMS ENFORCEMENT
AND CALIFORNIA DEPARTMENT OF JUSTICE,
CRIMINAL INTELLIGENCE BUREAU REGARDING
THE SHARING OF INFORMATION RELATING TO
CRIMINAL STREET GANGS**

- 1. PARTIES.** The parties to this Memorandum of Understanding (MOU) are the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), and the California Department of Justice, Criminal Intelligence Bureau (CIB) on behalf of the Executive Board (CEB) of the CALGANG® system.
- 2. AUTHORITY.** ICE is authorized to enter this MOU under the provisions of: 8 U.S.C. § 1103; 8 U.S.C. § 1226(c); 19 U.S.C. § 1589a; and 5 U.S.C. § 552a(b)(3). The California DOJ is authorized to enter this MOU under the provisions of California Government Code sections 15025-15027.
- 3. PURPOSE.** The purpose of this MOU is to set forth terms by which ICE and CIB are to share law enforcement intelligence relating to criminal street gangs.
- 4. DEFINITIONS:**

CALGANG®: Database maintained by the California Department of Justice for tracking gang-related criminal intelligence.

GANGNET®: Generic gang database software platform that replicates the CALGANG® database.

CEB: CALGANG® Executive Board

CGNAC: California Gang Node Advisory Committee

Criminal Intelligence Information: Information that has been evaluated and determined to be relevant to the identification of and/or activities of an individual or organization reasonably suspected of involvement in definable criminal activity.

Node: Independent repository of electronic gang-related data within GANGNET® for which an agency (Federal, state, or local) is responsible for maintaining. Such responsibility includes the addition, deletion, altering, and correction of information contained in that agency's node.

5. RESPONSIBILITIES:

ICE will:

- a. Establish procedures to provide California DOJ "read-only" access to the ICE GANGNET© database.
- b. Identify ICE personnel, and provide required training to such personnel, who will be authorized to have read only access to and utilization of the CALGANG© database. Training is to consist of a course of instruction at the Train-the-Trainer and User levels that address, at a minimum:
 - i. The definition of a criminal street gang;
 - ii. Accepted criteria for identifying gang members, associates, and entry of photographs;
 - iii. Criminal predicate/reasonable suspicion definitions;
 - iv. Federal, state, and local statutes and policies regarding criminal intelligence information; and
 - v. Responsibilities related to, and utilization of the CALGANG© system.
- c. Initiate procedures to resolve ICE internal network issues and difficulties related to the utilization of the CALGANG © system;
- d. Initiate procedures to acquire, install, maintain and utilize dedicated circuits for connectivity to the CALGANG© database, as well as acquiring appropriate hardware to connect to CALGANG© database;
- e. Initiate procedures to ensure that ICE personnel authorized to utilize the CALGANG© database have the appropriate level ICE background investigation and security clearance;
- f. Ensure compliance with all provisions of 28 C.F.R. § 23 that apply to ICE, including, but not limited to, the record validation and retention provisions contained in 28 § 23.20(g) and (h) as well as the dissemination provisions contained in 28 CFR. § 23.20(e) and (f).
- g. Setup primary points of contact between ICE and California DOJ, establish procedures and provide information developed by ICE through the comparison of CALGANG© data to ICE data to CALGANG© through the California DOJ node.
- h. Establish procedures and develop criteria for identifying and documenting criminal gang members based on input from the ICE field offices. Such

criteria are to be compatible with CGNAC Policy and Procedure provisions dealing with entry criteria.

1. Establish procedures to conduct periodic routine audits of the ICE system consistent with existing procedures and standards that will be developed in conjunction with the CGNAC, or when such a review is deemed warranted by ICE for system security purposes;

California DOJ will:

- a. Work with CEB and CGNAC to establish procedures to provide ICE "read-only" access to its CALGANG© database.
- b. Initiate procedures to resolve all internal CIB network issues and difficulties, including issues relating to the maintenance of the CALGANG© database, troubleshooting, and connectivity to support ICE utilization of the system;
- c. Setup primary points of contact between ICE and California DOJ, and establish procedures to provide ICE with Technical and Business Subject Matter Experts (SME's) to facilitate the exchange of technical information and technical support related to infrastructure(s), configuration(s), and security on an as needed basis to support ICE's utilization of the CALGANG © system;
- d. Provide ICE with information and standards regarding communications security procedures and protocols to ensure technical communications connectivity for the protection of information (data) and the respective ICE and CALGANG © systems.

6. POINTS OF CONTACT.

- a. For ICE: Unit Chief, Human Rights Violators and Public Safety Unit, Office of Investigations.
- b. For CIB: (1) the chairperson of CGNAC and (2) the person acting as the Chief of the DOJ/CIB.

7. TREATMENT OF INFORMATION SHARED

The Parties agree that subsequent uses and treatment of information (including data) shared under this MOU are restricted by the following conditions:

- a. Information is shared between the Parties pursuant to an express understanding of confidentiality. Such information, as well as inquiries and requests for information, received by a Party under this MOU, is to be accorded protection

from disclosure to third parties to the greatest extent permissible under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and subject to disclosure restrictions contained in the Privacy Act (PA), 5 U.S.C. § 552a, and California Government Code sections 6250, et seq. (the California Public Records Act); California Civil Code sections 1798, et seq. (the California Information Practices Act) as limited by California Penal Code sections 11105, 11120, et seq. 13102 and 13300 et seq., and California Evidence Code section 1040;

- b. The information available to the Parties through each Party's respective Node is to be treated as law enforcement intelligence and is not to be used as evidence in any criminal, civil or administrative proceeding, nor is it to be used independently as probable cause to support arrest, search, seizure or another law enforcement action. The Parties may only use source documentation to support legal proceedings and must confirm information contained in records with the source agency to support any law enforcement action.
- c. A Party that has received information from the other Party pursuant to this MOU is not to use or disclose such information except for the purposes enumerated herein, or as otherwise agreed to by the Party that was the source of the information;
- d. In the event that ICE receives a FOIA or PA request for information, Congressional inquiry, or other request for information the response to which requires disclosure of records obtained from CIB, or analytical product based thereon, ICE is to consult with CIB prior to responding to the requester and protect such information from the disclosure to the greatest extent permissible under applicable laws;
- e. In the event CIB receives a request for information from a non-law enforcement State government entity, or pursuant to any State of California information disclosure laws, where information requested includes ICE records or any analytical product based thereon, CIB is to consult with ICE prior to responding to the requester and protect such information from disclosure to the greatest extent permissible under applicable laws;
- f. The Parties are to obtain permission for the disclosure to third parties of information received pursuant to this MOU prior to such disclosure; unless there is a compelling need that would justify a Party's not making such a request, in which case the Party seeking to disclose the information is to give notice of the disclosure to the Party that was the source of the information as soon as practicable. A compelling need exists where there is a necessity to disclose the information in order to avoid imminent danger to life or property;

- g. To the extent either Party discloses information received under this MOU to a government entity in accordance with paragraphs 7d and 7e, the Party is to provide notice to the third party to which the information was disclosed that the third party is prohibited from further disclosure unless it obtains authorization from the Party that was the source of the information;
- h. To prevent the unauthorized disclosure, copying, use, or modification of information provided to a Party under this MOU, the receiving Party is to restrict access to such information on a need to know basis where such access is permitted by law and consistent with internal policy, and use recognized security mechanisms such as passwords, encryption, or other reasonable safeguards to prevent unauthorized access;
- i. Prior to releasing any information to the media regarding any prosecution, investigation, or other enforcement action based on information developed under this MOU, the Parties are to confer in order to ensure that the information to be released is accurate and may otherwise be properly disclosed.

8. OTHER PROVISIONS.

- a. Nothing in this MOU is intended to conflict with current law, regulation, policy, or the directives of ICE, CIB, CEB or CGNAC. If a term of this agreement is inconsistent with such authority, then the term shall be invalid, but the remaining terms and conditions of this agreement shall remain in full force and effect.
- b. This MOU is an internal arrangement between ICE and CIB and does not create or confer any right or benefit on any other person or party, private or public.
- c. Each Party is responsible for any expenses it incurs as a result of activities under this MOU.

9. EFFECTIVE DATE. The terms of this agreement will become effective upon signature by both parties.

10. DURATION.

The terms of this MOU will become effective upon the signature of both Parties. This MOU will remain in force as long as needed for the benefit of ICE, CEB and CGNAC.

11. MODIFICATION.

This MOU may be modified upon the mutual written consent of the Parties.

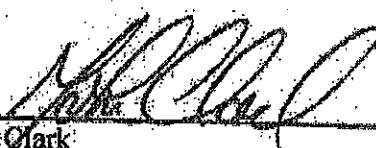
12. REVIEW.

This MOU will be subject to an initial review six months after its effective date, and every two years thereafter. Failure of the parties to conduct periodic reviews will not result in the termination of activities provided for under this MOU.

13. TERMINATION.

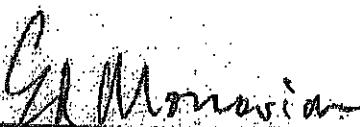
Either Party, upon 90 days written notice to the other Party, may terminate this MOU.

APPROVED BY:


John P. Clark
Acting Assistant Secretary
Immigration and Customs Enforcement
Department of Homeland Security

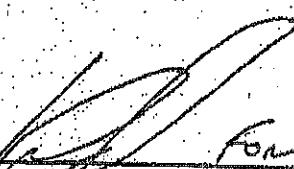
1-3-06

Date


Ed Manavian, Chief
State of California, Department of Justice
Criminal Intelligence Bureau

10/17/05

Date


Rick Oulets, Director
State of California, Department of Justice
Division of Law Enforcement

11/3/05

Date


Jim Lombard, Deputy Director
State of California, Department of Justice
Administrative Services Division

12/2/2005

Date

MEMORANDUM OF UNDERSTANDING BETWEEN
THE FEDERAL BUREAU OF INVESTIGATION,
AND THE CALIFORNIA DEPARTMENT OF JUSTICE,
BUREAU OF INVESTIGATION REGARDING
THE SHARING OF INFORMATION RELATING TO
CRIMINAL STREET GANGS

1. PARTIES. The parties to this Memorandum of Understanding (MOU) are the Federal Bureau of Investigation (FBI) and the California Department of Justice, Criminal Intelligence Bureau (CIB), acting on behalf of the Executive Committee (CEB) of the CalGang System.
2. AUTHORITY. The FBI is authorized to enter this MOU under the provisions of: 28 U.S.C. 533, 28 U.S.C. 534, 28 CFR 0.85 and 5 U.S.C. 552a. The California DOJ is authorized to enter this MOU under the provisions of California Government Code sections 15025-15027.
3. PURPOSE. The purpose of this MOU is to set forth terms by which the FBI and CIB are to share law enforcement intelligence relating to criminal street gangs.
4. DEFINITIONS:

CALGANG®: A database maintained by the California Department of Justice and operated in accordance with 28 CFR part 23 for the benefit of state and local California law enforcement agencies, the policies of which are determined by the CEB acting on its own initiative or in response to a recommendation from CGNAC.

CALGANG users: California state and local law enforcement agencies that utilize the CALGANG system.

GANGNET®: Generic gang database software platform that hosts the CALGANG® database.

CEB: CALGANG® Executive Board

CGNAC: California Gang Node Advisory Committee

Criminal Intelligence Information: Information which has been evaluated to determine that it is relevant to the identification of and the criminal activities engaged in by an individual who or organization which is reasonably suspected of involvement in criminal

activity, and, if the information pertains to political, religious or social views, associations or activities of such individuals or organizations that it is directly related to the suspected criminal activity.

Node: Independent repository of electronic gang-related data within GangNet® which an agency (Federal, state, or local) is responsible for maintaining. Such responsibility includes the addition, deletion, alteration, and correction of information contained in that agency's node.

5. RESPONSIBILITIES:

The FBI will:

- a. Establish procedures to provide CalGang Users, as defined herein, with "read only" access to the FBI GangNet node, once such node is developed.
- b. Identify FBI personnel, and provide training to such personnel, who will be authorized to have "read only" access to the CALGANG® database. Training is to consist of a course of instruction at the Train-the-Trainer and User levels that address, at a minimum:
 - i. The definition of a criminal street gang;
 - ii. Accepted criteria for identifying gang members, associates, and entry of photographs;
 - iii. Criminal predicate/reasonable suspicion definitions;
 - iv. Federal, state, and local statutes and policies regarding criminal intelligence information; and
 - v. Responsibilities related to, and utilization of the CALGANG® system.
- c. Initiate procedures to resolve the FBI internal network issues and difficulties related to the utilization of the CALGANG® system;
- d. Initiate procedures to acquire, install, maintain and utilize dedicated circuits for connectivity to the CALGANG® database, as well as acquiring appropriate hardware to connect to the CALGANG® database;
- e. Initiate procedures to ensure that FBI personnel authorized to utilize the CALGANG® database have the appropriate level of FBI background investigation and security clearance;
- f. Ensure compliance with all provisions of 28 C.F.R. part 23 that apply to the FBI, including, but not limited to, the record validation and retention provisions contained in 28

C.E.R. §§ 23.20(g) and (h) as well as the dissemination procedures contained in 28 C.F.R. §§ 23.20(e) and (f).

- g. Set up primary points of contact between the FBI and California DOJ. Establish procedures and provide information developed by the FBI, through the comparison of CALGANG© data to the FBI data, to CalGang through the California DOJ.
- h. Establish procedures and develop criteria for identifying and documenting criminal gang members based on input from FBI field offices. Such criteria are to be compatible with CGNAC Policy and Procedures provisions dealing with entry criteria.
- i. Establish procedures to conduct periodic routine audits of the FBI system consistent with existing CIB procedures and standards that will be developed in conjunction with the CGNAC, or when such a review is deemed warranted by the FBI for system security purposes;

CIB will:

- a. Work with CEB and CGNAC to establish procedures to provide the FBI with "read-only" access to its CALGANG© database.
- b. Initiate procedures to resolve all internal CIB network issues and difficulties, including issues relating to the maintenance of the CALGANG© database, troubleshooting, and connectivity to support FBI utilization of the system;
- c. Setup primary points of contact between the FBI and CIB, and establish procedures to provide the FBI with Technical and Business Subject Matter Experts (SME's) to facilitate the exchange of technical information and technical support related to infrastructure(s), configuration(s), and security on an as needed basis to support the FBI's utilization of the CALGANG© system;
- d. Provide the FBI with information and standards regarding communications security procedures and protocols to ensure technical communications connectivity for the protection of information (data) and the respective FBI and CALGANG© systems.

6. POINTS OF CONTACT.

- a. For the FBI: Chief National Gang Intelligence Center (NGIC), Criminal Division, FBI Headquarters, Washington, DC.

b. For CIB: (1) The Chairperson of CGNAC and (2) the person acting as the Chief of DOJ/CIB.

7. ACCESS TO AND USE OF INFORMATION

The Parties agree to the following conditions with regard to use and treatment of the information (including data) shared under this MOU:

- a. Information is shared between the Parties pursuant to an express understanding of confidentiality. Such information, as well as inquiries and requests for information, received by a Party under this MOU, is to be accorded protection from disclosure to third parties to the greatest extent permissible under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and subject to disclosure restrictions contained in the Privacy Act (PA), 5 U.S.C. § 552a, and California Government Code sections 6250, et seq. (the California Public Records Act); California Civil Code sections 1798, et seq. (the California Information Practices Act) as limited by California Penal Code Sections 11105, 11120, et seq. 13102 and 13300 et seq., and California Evidence Code section 1040;
- b. The information available to the Parties through each Parties' respective Node is to be treated as law enforcement intelligence and is not to be used as evidence in any criminal, civil, or administrative proceeding, nor is it to be used independently to establish probable cause for an arrest or a search with or without a warrant, or to support any other law enforcement action. The Parties may only use source documentation to support legal proceedings and/or law enforcement action and must confirm information contained in records with and request permission from the source agency prior to any such use of the information;
- c. A Party that has received information from the other Party pursuant to this MOU is not to use or disclose such information except for the purposes enumerated herein, or as otherwise agreed to by the Party that was the source of the information;
- d. In the event the FBI receives a FOIA or PA request for information, Congressional inquiry, or other request for information the response to which requires disclosure of records obtained from CIB, or any analytical product based thereon, the FBI is to consult with CIB prior to responding to the requester and will protect such information from disclosure to the greatest extent permissible under applicable laws.

- c. In the event CIB receives a request for information from a non-law enforcement State government entity, or pursuant to any State of California information disclosure laws, where information requested includes any FBI records or any analytical product based thereon, CIB is to consult with the FBI prior to responding to the requestor and protect such information from disclosure to the greatest extent possible under applicable laws.
- f. The Parties are to obtain permission for the disclosure to third parties of information received pursuant to this MOU prior to such disclosure, unless there is a compelling need that would justify a Party's not making such a request, in which case the Party seeking to disclose the information is to give notice of the disclosure to the Party that was the source of the information as soon as practicable. A compelling need exists when there is a necessity to disclose the information in order to avoid imminent danger to life or property.
- g. To the extent either Party discloses information received under this MOU to a government third party in accordance with the provisions of this MOU, the Party is to provide notice to the third party to which the information was disclosed that the third party is prohibited from further disclosure unless it obtains authorization from the Party that was the source of the information;
- h. To prevent the unauthorized disclosure, copying, use, or modification of information provided to a Party under this MOU, the receiving Party is to restrict access to such information on a need to know basis, and use recognized security mechanisms such as passwords, encryption, or other reasonable safeguards to prevent unauthorized access;
- i. Prior to releasing any information to the media regarding any prosecution, investigation, or other enforcement action based on information developed under this MOU, the Parties are to confer in order to ensure that the information to be released is accurate and may otherwise be properly disclosed.

8. OTHER PROVISIONS.

- a. Nothing in this MOU is intended to conflict with current law, regulation, policy, or the directives of the FBI, or CIB, CEB or CGNAC. If a term of this agreement is inconsistent with such authority, then the term shall be invalid, but the remaining terms and conditions of this agreement shall remain in full force and effect.

- b. This MOU is an internal arrangement between the FBI and CIB and does not create or confer any right or benefit on any other person or party, private or public.
- c. Unless otherwise provided herein or in a supplementary writing, each party shall bear its own costs in relation to this MOU. Even where a party has agreed (or later does agree) to assume a particular financial responsibility, the party's express written approval must be obtained before the incurring by another party of each expense associated with the responsibility. All obligations of and expenditures by the parties will be subject to their respective budgetary and fiscal processes and availability of funds pursuant to all laws, regulations, and policies applicable thereto. The parties acknowledge that there is no intimation, promise, or guarantee that funds will be available in future years.

9. EFFECTIVE DATE.

The terms of this agreement will become effective upon a signature by both parties.

10. DURATION

The terms of this MOU shall remain in force as long as needed for the benefit of the FBI, CIB, CEB, and CGNAC. This MOU will be the subject of an initial review six months after its effective date and every two years thereafter. Failure of the parties to conduct periodic reviews will not result in the termination of activities provided for under this MOU.

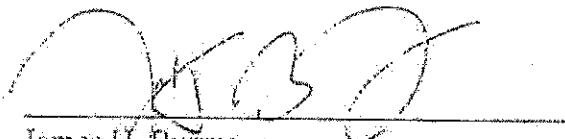
11. MODIFICATION.

This MOU may be modified upon the mutual written consent of the Parties.

12. TERMINATION.

Either Party, upon 90 days written notice to the other Party, may terminate this MOU. All rights, obligations, responsibilities, limitations, and other understandings with respect to the disclosure and use of information received during a Parties' participation in this MOU shall survive any termination.

APPROVED BY:



James H. Burrus
Acting Assistant Director
Criminal Division
Federal Bureau of Investigation



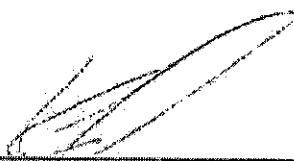
Craig Buehler
Chief
Criminal Intelligence Bureau
California Department of Justice

7/9/06
(date)

8/8/06
(date)

Memorandum of Understanding Between The Federal Bureau of Investigation,
And the California Department of Justice, Criminal Intelligence Bureau
regarding the Sharing of Information Relating to Criminal Street Gangs

Signatories



Wilfredo Cid, Assistant Director
State of California, Department of Justice
Division of Law Enforcement



Date



Jim Lombard, Deputy Director
State of California, Department of Justice
Administrative Services Division



Date